

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-366519

(P2002-366519A)

(43) 公開日 平成14年12月20日 (2002. 12. 20)

(51) Int.Cl.⁷

G 0 6 F 15/00

H 0 4 L 9/32

識別記号

3 3 0

F I

G 0 6 F 15/00

H 0 4 L 9/00

ターム(参考)

3 3 0 B 5 B 0 8 5

6 7 3 A 5 J 1 0 4

6 7 3 B

6 7 5 D

審査請求 未請求 請求項の数4 O L (全 8 頁)

(21) 出願番号 特願2001-174593(P2001-174593)

(22) 出願日 平成13年6月8日(2001. 6. 8)

(71) 出願人 392026693

株式会社エヌ・ティ・ティ・ドコモ
東京都千代田区永田町二丁目11番1号

(72) 発明者 飯田 政也

東京都千代田区永田町二丁目11番1号 株
式会社エヌ・ティ・ティ・ドコモ内

(74) 代理人 100088155

弁理士 長谷川 芳樹 (外4名)

Fターム(参考) 5B085 AE03 AE04 AE23

5J104 AA07 AA16 EA03 EA16 KA01

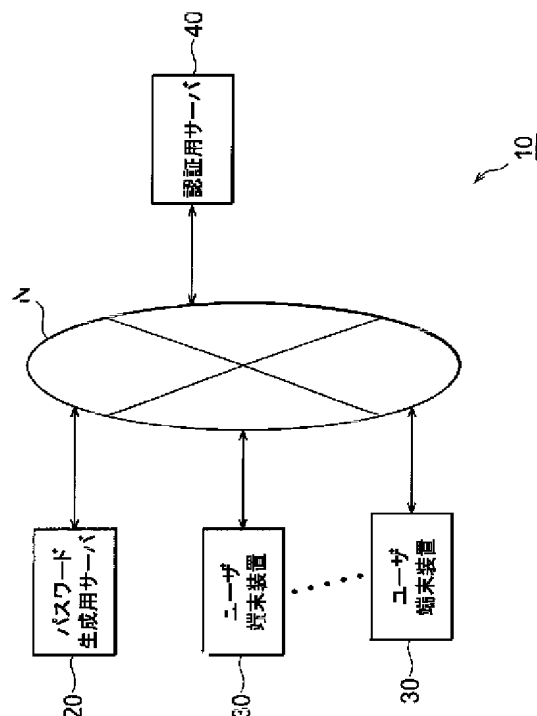
KA02 KA21 MA02 NA05 PA07

(54) 【発明の名称】 電子認証システム及び電子認証方法

(57) 【要約】

【課題】 導入、維持するための費用を低くすることができ、管理を容易に行うことが可能な電子認証システム及び電子認証方法を提供すること。

【解決手段】 パスワード生成用サーバ20は、複数のユーザ端末装置30毎にパスワードを生成し、生成したパスワードを複数のユーザ端末装置30に一斉送信する。また、パスワード生成用サーバ20は、生成したパスワードと当該パスワードを送信するユーザ端末装置30を特定するための識別子とを認証用サーバ40に送信する。ユーザ端末装置30は、認証を得るために、パスワード生成用サーバ20から送信されたパスワードとユーザ端末装置30の識別子とを認証用サーバ40に送信する。認証用サーバ40は、ユーザ端末装置30から送信されたパスワードとユーザ端末装置30の識別子と、パスワード情報格納部に格納されたパスワードと識別子とを照合し、ユーザ端末装置30の認証を行う。



【特許請求の範囲】

【請求項1】 複数のユーザ端末装置と認証用サーバとがネットワークを介して接続されており、前記認証用サーバがそれぞれの前記ユーザ端末装置から送信されたパスワードを照合して当該ユーザ端末装置の認証を行う電子認証システムであって、
前記複数のユーザ端末装置毎にパスワードを生成するパスワード生成手段と、前記パスワード生成手段にて生成された前記パスワードを前記複数のユーザ端末装置に一齐送信するパスワード送信手段と、前記パスワード生成手段にて生成された前記パスワードと当該パスワードが送信されるユーザ端末装置を特定するための識別子とを前記認証用サーバに送信するパスワード情報送信手段と、を有するパスワード生成用サーバを備えており、
前記ユーザ端末装置のそれぞれは、前記パスワード送信手段から一齐送信された前記パスワードと当該ユーザ端末装置を特定するための識別子とを前記認証用サーバに送信するユーザ情報送信手段を有し、
前記認証用サーバは、前記パスワード情報送信手段から送信された前記パスワードと前記ユーザ端末装置を特定するための識別子とを格納するパスワード情報格納手段と、前記ユーザ情報送信手段から送信された前記パスワードと前記ユーザ端末装置を特定するための識別子と、前記パスワード情報格納手段に格納された前記パスワードと前記ユーザ端末装置を特定するための識別子とを照合して前記ユーザ端末装置の認証を行う照合手段と、を有していることを特徴とする電子認証システム。

【請求項2】 前記パスワード生成手段は、前記パスワードを周期的に更新するように生成しており、
前記パスワード情報送信手段は、前記パスワード送信手段から前記複数のユーザ端末装置に前記パスワードを一齐送信した時間を特定するための時間情報を前記認証用サーバに更に送信し、
前記パスワード情報格納手段は、前記パスワード情報送信手段から送信された前記時間情報を更に格納し、
前記照合手段は、前記ユーザ情報送信手段から前記パスワードが送信された時間と、前記パスワード情報格納手段に格納された前記時間情報とを更に照合することを特徴とする請求項1に記載の電子認証システム。

【請求項3】 複数のユーザ端末装置と認証用サーバとがネットワークを介して接続されており、前記認証用サーバがそれぞれの前記ユーザ端末装置から送信されたパスワードを照合して当該ユーザ端末装置の認証を行う電子認証方法であって、
パスワード生成用サーバが、前記複数のユーザ端末装置毎にパスワードを生成するパスワード生成ステップと、
前記パスワード生成用サーバが、前記パスワード生成ステップにて生成された前記パスワードを前記複数のユーザ端末装置に一齐送信するパスワード送信ステップと、
前記パスワード生成用サーバが、前記パスワード生成ス

テップにて生成された前記パスワードと当該パスワードが送信されるユーザ端末装置を特定するための識別子とを前記認証用サーバに送信するパスワード情報送信ステップと、
前記ユーザ端末装置が、前記パスワード送信ステップにて一齐送信された前記パスワードと当該ユーザ端末装置を特定するための識別子とを前記認証用サーバに送信するユーザ情報送信ステップと、
前記認証用サーバが、前記パスワード情報送信ステップにて送信された前記パスワードと前記ユーザ端末装置を特定するための識別子とをパスワード情報格納手段に格納するパスワード情報格納ステップと、
前記認証用サーバが、前記ユーザ情報送信ステップにて送信された前記パスワードと前記ユーザ端末装置を特定するための識別子と、前記パスワード情報格納手段に格納された前記パスワードと前記ユーザ端末装置を特定するための識別子とを照合して前記ユーザ端末装置の認証を行う照合ステップと、を有していることを特徴とする電子認証方法。

【請求項4】 前記パスワード生成ステップでは、前記パスワード生成用サーバが、前記パスワードを周期的に更新するように生成しており、
前記パスワード情報送信ステップでは、前記パスワード生成用サーバが、前記パスワード送信手段から前記複数のユーザ端末装置に前記パスワードを一齐送信した時間を特定するための時間情報を前記認証用サーバに更に送信し、
前記パスワード情報格納ステップでは、前記認証用サーバが、前記パスワード情報送信手段から送信された前記時間情報を前記パスワード情報格納手段に更に格納し、
前記照合ステップでは、前記認証用サーバが、前記ユーザ端末装置から前記パスワードが送信された時間と、前記パスワード情報格納手段に格納された前記時間情報とを更に照合することを特徴とする請求項3に記載の電子認証方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数のユーザ端末装置とネットワークを介して接続された認証用サーバが、それぞれのユーザ端末装置から送信されたパスワードを照合して当該ユーザ端末装置の認証を行う電子認証システム及び電子認証方法に関する。

【0002】

【従来の技術】この種の電子認証システム及び電子認証方法として、ワンタイムパスワード方式がある。このワンタイムパスワード方式では、認証の度毎に新しいパスワードを利用して認証を行うため、仮にパスワードが第三者に漏洩しても最小限の被害に食い止めることができる。ワンタイムパスワード方式を採用した従来技術においては、認証用サーバと同期して、生成するパスワード

を認証の度毎に変更していくワンタイムパスワード生成器を用いている。認証用サーバに認証を要求する際、ユーザは、ワンタイムパスワード生成器が生成したワンタイムパスワードをユーザ自身のIDと共に認証用サーバに送信する。認証用サーバはワンタイムパスワード生成器と同期しているので、認証要求を受けた時点で該IDに対応するワンタイムパスワードを生成することができる。よって、認証用サーバはユーザから受け取ったワンタイムパスワードと認証用サーバ自身が生成したワンタイムパスワードを比較してユーザを認証することができる。

【0003】

【発明が解決しようとする課題】上述のワンタイムパスワード方式を用いた従来技術では、専用のハードウェア、あるいは、専用のソフトウェアとこれを実行可能なハードウェアとして、認証用サーバと同期してワンタイムパスワードを生成するワンタイムパスワード生成器を、すべてのユーザに対して準備する必要がある。このため、電子認証システム（電子認証方法）を導入、維持するための費用が高くなってしまう。

【0004】また、ユーザがワンタイムパスワード生成器を紛失、あるいは盗まれた場合には、紛失あるいは盗まれたワンタイムパスワード生成器を取得した第三者が認証用サーバにアクセスするのを防ぐために、当該ワンタイムパスワード生成器から送信されるワンタイムパスワードを無効にする等の対策が必要となる。また、ワンタイムパスワード生成器を紛失、あるいは盗まれたユーザに対して、新たなワンタイムパスワード生成器を供給する必要がある。このように、ワンタイムパスワード生成器を用いた場合、電子認証システムを適切に運用するための管理が複雑なものになってしまう。

【0005】そこで、本発明は、上記問題点を解決し、導入、維持するための費用を低くすることができ、管理を容易に行うことが可能な電子認証システム及び電子認証方法を提供することを課題とする。

【0006】

【課題を解決するための手段】本発明に係る電子認証システムは、複数のユーザ端末装置と認証用サーバとがネットワークを介して接続されており、認証用サーバがそれぞれのユーザ端末装置から送信されたパスワードを照合して当該ユーザ端末装置の認証を行う電子認証システムであって、複数のユーザ端末装置毎にパスワードを生成するパスワード生成手段と、パスワード生成手段にて生成されたパスワードを複数のユーザ端末装置に一斉送信するパスワード送信手段と、パスワード生成手段にて生成されたパスワードと当該パスワードが送信されるユーザ端末装置を特定するための識別子とを認証用サーバに送信するパスワード情報送信手段と、を有するパスワード生成用サーバを備えており、ユーザ端末装置のそれぞれは、パスワード送信手段から一斉送信されたパスワ

ードと当該ユーザ端末装置を特定するための識別子とを認証用サーバに送信するユーザ情報送信手段を有し、認証用サーバは、パスワード情報送信手段から送信されたパスワードとユーザ端末装置を特定するための識別子とを格納するパスワード情報格納手段と、ユーザ情報送信手段から送信されたパスワードとユーザ端末装置を特定するための識別子と、パスワード情報格納手段に格納されたパスワードとユーザ端末装置を特定するための識別子とを照合してユーザ端末装置の認証を行う照合手段と、を有していることを特徴としている。

【0007】一方、本発明に係る電子認証方法は、複数のユーザ端末装置と認証用サーバとがネットワークを介して接続されており、認証用サーバがそれぞれのユーザ端末装置から送信されたパスワードを照合して当該ユーザ端末装置の認証を行う電子認証方法であって、パスワード生成用サーバが、複数のユーザ端末装置毎にパスワードを生成するパスワード生成ステップと、パスワード生成用サーバが、パスワード生成ステップにて生成されたパスワードを複数のユーザ端末装置に一斉送信するパスワード送信ステップと、パスワード生成用サーバが、パスワード生成ステップにて生成されたパスワードと当該パスワードが送信されるユーザ端末装置を特定するための識別子とを認証用サーバに送信するパスワード情報送信ステップと、ユーザ端末装置が、パスワード送信ステップにて一斉送信されたパスワードと当該ユーザ端末装置を特定するための識別子とを認証用サーバに送信するユーザ情報送信ステップと、認証用サーバが、パスワード情報送信ステップにて送信されたパスワードとユーザ端末装置を特定するための識別子とをパスワード情報格納手段に格納するパスワード情報格納ステップと、認証用サーバが、ユーザ情報送信ステップにて送信されたパスワードとユーザ端末装置を特定するための識別子とを照合してユーザ端末装置の認証を行う照合ステップと、を有していることを特徴としている。

【0008】これら、本発明に係る電子認証システム及び電子認証方法それぞれによれば、パスワード生成用サーバにて、パスワードが複数のユーザ端末装置毎に生成され、生成されたパスワードが複数のユーザ端末装置に一斉送信されると共に、生成されたパスワードと当該パスワードが送信されるユーザ端末装置を特定するための識別子とが認証用サーバに送信される。そして、認証用サーバにて、ユーザ端末装置から送信されたパスワードとユーザ端末装置を特定するための識別子と、パスワード情報格納手段に格納されたパスワードとユーザ端末装置を特定するための識別子とが照合されてユーザ端末装置の認証が行われる。このように、認証用サーバにて、パスワード生成用サーバにて生成されたパスワードに基づいてユーザ端末装置の認証が行われることになるの

で、それぞれのユーザに対してワンタイムパスワード生成器等の専用ハードウェアが必要とされる従来の技術に比して、電子認証システム（電子認証方法）を導入、維持するための費用を低くできる。

【0009】また、本発明によれば、ユーザがユーザ端末装置を紛失、あるいは盗まれた場合において、ユーザがパスワードの送信先を変更することにより、紛失あるいは盗まれたユーザ端末装置を取得した第三者が認証用サーバにアクセスするのを簡易に防ぐことができ、電子認証システム（電子認証方法）を適切に運用するための管理を容易に行うことができる。

【0010】また、本発明に係る電子認証システムにおいては、パスワード生成手段は、パスワードを周期的に更新するように生成しており、パスワード情報送信手段は、パスワード送信手段から複数のユーザ端末装置にパスワードを一斉送信した時間を特定するための時間情報を認証用サーバに更に送信し、パスワード情報格納手段は、パスワード情報送信手段から送信された時間情報を更に格納し、照合手段は、ユーザ情報送信手段からパスワードが送信された時間と、パスワード情報格納手段に格納された時間情報とを更に照合することが好ましい。

【0011】一方、本発明に係る電子証明書発行管理方法においては、パスワード生成ステップでは、パスワード生成用サーバが、パスワードを周期的に更新するように生成しており、パスワード情報送信ステップでは、パスワード生成用サーバが、パスワード送信手段から複数のユーザ端末装置にパスワードを一斉送信した時間を特定するための時間情報を認証用サーバに更に送信し、パスワード情報格納ステップでは、認証用サーバが、パスワード情報送信手段から送信された時間情報をパスワード情報格納手段に更に格納し、照合ステップでは、認証用サーバが、ユーザ端末装置からパスワードが送信された時間と、パスワード情報格納手段に格納された時間情報とを更に照合することが好ましい。

【0012】このように構成した場合、それぞれにおいて、パスワード生成用サーバにて周期的に更新するように生成されたパスワードに基づいてユーザ端末装置の認証が行われることになるので、認証用サーバにて行われるユーザ端末装置の認証の信頼性を向上することができる。また、パスワードの更新周期の変更を容易に行うことができる。

【0013】

【発明の実施の形態】以下、図面を参照しながら本発明による電子認証システム及び電子認証方法の好適な実施形態について詳細に説明する。

【0014】まず、本実施形態に係る電子認証システムの構成について説明する。図1は、本実施形態に係る電子認証システムの構成図である。本実施形態にかかる電子認証システム10は、図1に示すように、パスワード生成用サーバ20と、複数のユーザ端末装置30と、認

証用サーバ40とを備えて構成される。これらのパスワード生成用サーバ20、ユーザ端末装置30、及び、認証用サーバ40は、ネットワークNを介して接続されている。

【0015】パスワード生成用サーバ20は、複数のユーザ端末装置毎にパスワードを生成し、送信する情報処理装置であって、物理的には、CPU（中央処理装置）、メモリ、マウスやキーボードなどの入力装置、ディスプレイなどの表示装置、ハードディスクなどの格納装置、モデムなどの送受信装置などを備えたコンピュータシステム（例えばパーソナルコンピュータ）として構成される。

【0016】複数のユーザ端末装置30それぞれは、ユーザが利用する端末装置であって、物理的には、ポケットベル（登録商標）（ページャ）、携帯電話等の携帯情報端末として構成される。ユーザ端末装置30がポケットベル、携帯電話等である場合には、ネットワークNは、ポケットベル、携帯電話等に対してデータを送受信するための無線伝送路を含むように構成される。なお、ユーザ端末装置30は、CPU（中央処理装置）、メモリ、マウスやキーボードなどの入力装置、ディスプレイなどの表示装置、ハードディスクなどの格納装置、モデムなどの送受信装置などを備えたコンピュータシステム（例えばパーソナルコンピュータ）として構成してもよい。

【0017】認証用サーバ40は、ユーザ端末装置30から送信されたパスワードを照合して当該ユーザ端末装置30の認証を行う情報処理装置であって、物理的には、CPU（中央処理装置）、メモリ、マウスやキーボードなどの入力装置、ディスプレイなどの表示装置、ハードディスクなどの格納装置、モデムなどの送受信装置などを備えたコンピュータシステム（例えばパーソナルコンピュータ）として構成される。

【0018】続いて、図2に基づいて、パスワード生成用サーバ20の構成について詳細に説明する。図2は、パスワード生成用サーバ20の機能を説明するためのブロック図である。パスワード生成用サーバ20は、機能的な構成要素として、パスワード生成部21（パスワード生成手段）と、パスワード送信部23（パスワード送信手段）と、パスワード情報送信部25（パスワード情報送信手段）とを備えて構成される。

【0019】パスワード生成部21は、複数のユーザ端末装置30毎にパスワードを生成する。本実施形態において、パスワード生成部21は、生成したパスワードを周期的に更新するように、所定時間（たとえば、4分）毎に新たなパスワードを生成している。パスワード送信部23は、パスワード生成部21にて生成されたパスワードを対応するユーザ端末装置30に一斉送信する。また、パスワード情報送信部25は、パスワード生成部21にて生成されたパスワードと、当該パスワードが送信

されるユーザ端末装置30を特定するための識別子と、当該パスワードをパスワード送信部23からそれぞれのユーザ端末装置30に一斉送信した時間を特定するための時間情報とをパスワード情報として、認証用サーバ40に送信する。

【0020】次に、図3に基づいて、ユーザ端末装置30の構成について詳細に説明する。図3は、ユーザ端末装置30の機能を説明するためのブロック図である。ユーザ端末装置30それぞれの、機能的な構成要素として、パスワード受信部31（パスワード受信手段）と、パスワード格納部33（パスワード格納手段）と、識別子格納部35（識別子格納手段）と、ユーザ情報送信部37（ユーザ情報送信手段）とを備えて構成される。

【0021】パスワード受信部31は、パスワード生成用サーバ20（パスワード送信部23）から送信されたパスワードを受信し、識別子格納部35に送る。パスワード格納部33は、パスワード受信部31から受信したパスワードが送られ、当該パスワードを格納、記憶する。識別子格納部35は、ユーザ端末装置30を区別するためのユーザ端末装置固有の識別子を格納、記憶している。ユーザ情報送信部37は、ユーザによる操作に基づいて、パスワード格納部33から格納されているパスワードを読み出し、識別子格納部35から格納されている識別子を読み出し、これらのパスワードと識別子とをユーザ情報として認証用サーバ40に送信する。識別子格納部35に格納される識別子と、パスワード情報送信部25からパスワード情報として送信される識別子とは、同じものであってもよく、また、互に対応付けが可能なものであれば、同じものでなくてもよい。

【0022】次に、図4に基づいて、認証用サーバ40の構成について詳細に説明する。図4は、認証用サーバ40の機能を説明するためのブロック図である。認証用サーバ40は、機能的な構成要素として、パスワード情報受信部41（パスワード情報受信手段）と、パスワード情報格納部43（パスワード情報格納手段）と、ユーザ情報受信部45（ユーザ情報受信手段）と、照合部47（照合手段）とを備えて構成される。

【0023】パスワード情報受信部41は、パスワード生成用サーバ20（パスワード情報送信部25）から送信されたパスワード情報を受信し、パスワード情報格納部43に送る。パスワード情報格納部43は、パスワード情報受信部41から受信したパスワード情報が送られ、当該パスワード情報を格納、記憶する。パスワード情報格納部43は、パスワード情報データベースを有している。パスワード情報データベースは、パスワード生成部21にて生成されたパスワードと、当該パスワードが送信されるユーザ端末装置30を特定するための識別子と、当該パスワードをパスワード送信部23からそれぞれのユーザ端末装置30に一斉送信した時間を特定するための時間情報とが対応付けられて格納されている。

これにより、識別子を検索キーとして、対応するパスワード及び時間情報を検索して抽出することができる。

【0024】ユーザ情報受信部45は、ユーザ端末装置30（ユーザ情報送信部37）から送信されたユーザ情報を受信し、照合部47に送る。照合部47は、ユーザ情報受信部45から送られたユーザ端末装置30のパスワード及び識別子と、パスワード情報格納部43に格納されたパスワード及び識別子とを照合してユーザ端末装置30の認証を行う。

【0025】照合部47は、情報の照合を以下のようにして行う。照合部47は、ユーザ情報受信部45から送られたユーザ情報に含まれる識別子に対応するパスワード情報を、パスワード情報格納部43のパスワード情報データベースに格納された情報から検出する。このとき、照合部47は、ユーザ情報受信部45から送られたユーザ情報に含まれる識別子を検索キーとして、パスワード情報データベースの情報を検索し、対応するパスワード情報、すなわちパスワード生成用サーバ20から送信されたパスワードと、当該パスワードをパスワード生成用サーバ20からそれぞれのユーザ端末装置30に一斉送信した時間を特定するための時間情報とを検出する。

【0026】照合部47は、ユーザ情報受信部45から送られたユーザ端末装置30のパスワード及びユーザ端末装置30（ユーザ情報送信部37）から当該パスワードが送信された時間と、パスワード情報格納部43から検出したパスワードと時間情報とを対比、照合して、ユーザ端末装置30の認証を行う。ユーザ端末装置30から送信されたパスワード及び時間がパスワード情報格納部43から検出したパスワード及び時間情報と一致する場合には、照合部47は、ユーザ端末装置30の認証を許可する。一方、パスワード情報格納部43から対応するパスワード情報を検出することができない、あるいは、ユーザ端末装置30から送信されたパスワード及び時間がパスワード情報格納部43から検出したパスワード及び時間情報と一致しない場合には、照合部47は、ユーザ端末装置30の認証を許可しない。

【0027】続いて、図5及び図6に示すフローチャートを参照しながら、本実施形態に係る電子認証システムの動作（電子認証方法）について説明する。図5及び図6は、本実施形態に係る電子認証システムの動作（電子認証方法）を示すフローチャートである。

【0028】パスワード生成用サーバ20のパスワード生成部21は、複数のユーザ端末装置30毎にパスワードを生成する（S101：パスワード生成ステップ）。このとき、パスワード生成部21は、生成したパスワードを周期的に更新するように、所定時間毎に新たなパスワードを生成する。パスワード生成部21は、パスワード生成ステップ（S101）にて生成したパスワードをパスワード送信部23と、パスワード情報送信部25と

に送出する（S103）。

【0029】パスワード生成用サーバ20のパスワード送信部23は、パスワード生成ステップ（S101）にて生成されパスワード生成部21から送出されたパスワードを受領し（S201）、受領したパスワードを対応するそれぞれのユーザ端末装置30（パスワード受信部31）に一斉送信する（S203：パスワード送信ステップ）。

【0030】一方、パスワード生成用サーバ20のパスワード情報送信部25は、パスワード生成ステップ（S101）にて生成されパスワード生成部21から送出されたパスワードを受領し（S301）、受領したパスワードと、当該パスワードが送信されるユーザ端末装置30を特定するための識別子と、当該パスワードをパスワード送信部23からそれぞれのユーザ端末装置30に一斉送信した時間を特定するための時間情報とをパスワード情報として、認証用サーバ40（パスワード情報受信部41）に送信する（S303：パスワード情報送信ステップ）。

【0031】ユーザ端末装置30のパスワード受信部31は、パスワード生成用サーバ20（パスワード送信部23）から送信されたパスワードを受信し（S401）、パスワード格納部33に送出する（S403）。パスワード格納部33は、パスワード受信部31から送出されたパスワードを格納、記憶する（S501）。

【0032】認証用サーバ40のパスワード情報受信部41は、パスワード生成用サーバ20（パスワード情報送信部25）から送信されたパスワード情報を受信し（S601）、パスワード情報格納部43に送出する（S603）。

【0033】認証用サーバ40のパスワード情報格納部43は、パスワード情報受信部41から送出されたパスワード情報をパスワード情報データベースに格納、記憶する（S701：パスワード情報格納ステップ）。このとき、パスワード情報は、上述したように、パスワード生成用サーバ20（パスワード生成部21）にて生成されたパスワードと、当該パスワードが送信されるユーザ端末装置30を特定するための識別子と、当該パスワードをパスワード送信部23からそれぞれのユーザ端末装置30に一斉送信した時間を特定するための時間情報とが対応付けられて格納される。

【0034】ユーザが自己のユーザ端末装置30の認証を得ようとしてユーザ端末装置30にて所定の操作を行うと、ユーザ端末装置30のユーザ情報送信部37は、パスワード格納部33に格納されているパスワードを読み出し（S801）、識別子格納部35に格納されている識別子を読み出す（S803）。そして、ユーザ情報送信部37は、読み出したパスワード及び識別子をユーザ情報として認証用サーバ40（ユーザ情報受信部45）に送信する（S805：ユーザ情報送信ステッ

プ）。

【0035】認証用サーバ40のユーザ情報受信部45は、ユーザ端末装置30（ユーザ情報送信部37）から送信されたユーザ情報を受信し（S901）、照合部47に送出する（S903）。照合部47は、ユーザ情報受信部45から送出されたユーザ情報を受領する（S1001）。

【0036】認証用サーバ40の照合部47は、ユーザ端末装置30（ユーザ情報送信部37）から送出されたユーザ情報を受領すると、当該ユーザ情報に含まれる識別子に対応するパスワード情報、すなわちパスワード生成用サーバ20から送信されたパスワードと、当該パスワードをパスワード生成用サーバ20からそれぞれのユーザ端末装置30に一斉送信した時間を特定するための時間情報とを、パスワード情報格納部43のパスワード情報データベースに格納された情報から検出する（S1003）。そして、照合部47は、ユーザ情報受信部45から送られたユーザ端末装置30のパスワード及びユーザ端末装置30（ユーザ情報送信部37）から当該パスワードが送信された時間と、パスワード情報格納部43から検出したパスワードと時間情報とを対比、照合し、この照合結果に基づいてユーザ端末装置30の認証を行う（S1005：照合ステップ）。

【0037】このように、本実施形態によれば、パスワード生成用サーバ20にて、パスワードが複数のユーザ端末装置30毎に生成され、生成されたパスワードが複数のユーザ端末装置30に一斉送信されると共に、生成されたパスワードと当該パスワードが送信されるユーザ端末装置30を特定するための識別子とが認証用サーバ40に送信される。そして、認証用サーバ40にて、ユーザ端末装置30から送信されたパスワードとユーザ端末装置30を特定するための識別子と、パスワード情報格納部43に格納されたパスワードとユーザ端末装置30を特定するための識別子とが照合されてユーザ端末装置30の認証が行われる。したがって、認証用サーバ40にて、パスワード生成用サーバ20にて生成されたパスワードに基づいてユーザ端末装置30の認証が行われることになるので、それぞれのユーザに対してワンタイムパスワード生成器等の専用ハードウェアが必要とされる従来の技術に比して、電子認証システム10（電子認証方法）を導入、維持するための費用を低くできる。

【0038】また、本実施形態によれば、パスワード生成用サーバ20にて周期的に更新するように生成されたパスワードに基づいてユーザ端末装置30の認証が行われることになるので、認証用サーバ40にて行われるユーザ端末装置30の認証の信頼性を向上することができる。また、パスワードの更新周期の変更を容易に行うことができる。

【0039】本発明は、前述した実施形態に限定されるものではない。たとえば、本実施形態においては、パス

ワード生成用サーバ20は、ユーザ端末装置30と認証用サーバ40とを接続しているネットワークNを通して、ユーザ端末装置30にパスワードを送付しているが、別のネットワークを通してユーザ端末装置30にパスワードを送付するようにしてもよい。同様に、パスワード生成用サーバ20は、別のネットワークを通して認証用サーバ40にパスワード情報を送付するようにしてもよい。

【0040】

【発明の効果】以上、詳細に説明したように、本発明にあっては、認証用サーバにて、パスワード生成用サーバにて生成されたパスワードに基づいてユーザ端末装置の認証が行われることになる。この結果、本発明によれば、導入、維持するための費用を低くすることができ、管理を容易に行うことが可能な電子認証システム及び電子認証方法を提供することができる。

【図面の簡単な説明】

【図1】本発明の実施形態に係る電子認証システムの構成図である。

【図2】本発明の実施形態に係る電子認証システムに含まれる、パスワード生成用サーバの機能を説明するため

のブロック図である。

【図3】本発明の実施形態に係る電子認証システムに含まれる、ユーザ端末装置の機能を説明するためのブロック図である。

【図4】本発明の実施形態に係る電子認証システムの動作（電子認証方法）を示すフローチャートである。

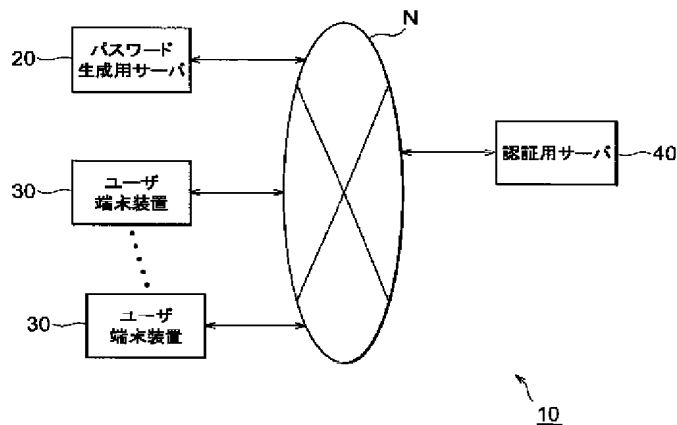
【図5】本発明の実施形態に係る電子認証システムの動作（電子認証方法）を示すフローチャートである。

【図6】本発明の実施形態に係る電子認証システムの動作（電子認証方法）を示すフローチャートである。

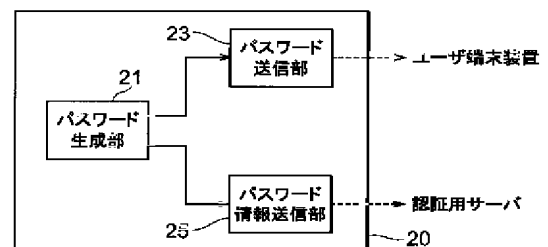
【符号の説明】

10…電子認証システム、20…パスワード生成用サーバ、21…パスワード生成部、23…パスワード送信部、25…パスワード情報送信部、30…ユーザ端末装置、31…パスワード受信部、33…パスワード格納部、35…識別子格納部、37…ユーザ情報送信部、40…認証用サーバ、41…パスワード情報受信部、43…パスワード情報格納部、45…ユーザ情報受信部、47…照合部、N…ネットワーク。

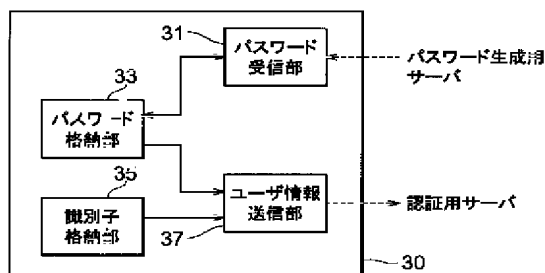
【図1】



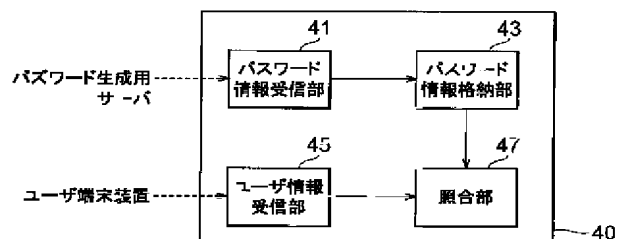
【図2】



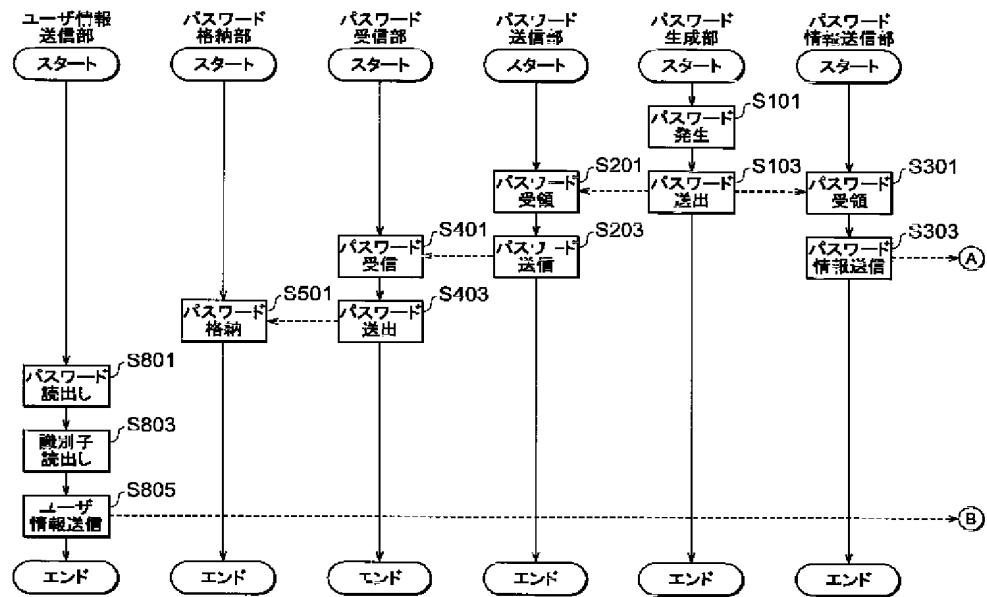
【図3】



【図4】



【図5】



【図6】

